CLAIMS

What is claimed is:

1. A method for generating keys for encoding data for transmission comprising:

accessing in a first device a device identification and at least one key corresponding to the device identification;

encoding data using the at least one key;

transmitting a message from the first device to the second device, the message comprising a header comprising the device identification and a data field comprising the encoded data;

said second device using the device identification received in the header of the message to determine the at least one key and decode the encoded data received in the data field of the message using the determined at least one key.

2. The method as set forth in claim 1, wherein the device identification is selected from the group consisting of a unique device identification of the first device, a unique device identification of the second device, a device address of the first device, and a device address of the second device.

3. The method as set forth in claim 1, wherein the at least one key is generated using the device identification and a plurality of generation keys.

4. The method as set forth in claim 3, further comprising generating the at least one key using a multistage process wherein a different generation key of the plurality of generation keys is used at each stage to operate with the output of a prior stage, a first stage having as input the device identification, and the a last stage outputting a key of the at least one key.

5. The method as set forth in claim 4, wherein each stage is selected from the group consisting of a cipher function, an Exclusive OR function, a mathematical

function, a logic function, a function that complies with the Advance Encryption Standard (AES), a function that complies with the Data Encryption Standard (DES) and functions that comply with determined encryption standards.

6. The method as set forth in claim 1, wherein the at least one key for encoding is selected from the group consisting of hashing and signing a message and encrypting a message.

7. The method as set forth in claim 1, wherein the device identification is selected from the group consisting of a unique network identification that is a mandatory part of a standard communication protocol, a unique device address, a unique device identification and a Media Access Control (MAC) address.

8. A communication device comprising:

a non-volatile storage medium for storing information for at least one key corresponding to a device identification of a communication device;

a first logic to encode data using the at least one key and decode encoded data using the at least one key;

an input/output to communicate encoded data in a message, the message including the device identification and the encoded data.

9. The device as set forth in claim 8, wherein a first communication device communicates with a second communication device and the device identification corresponds to the first communication device.

10. The device as set forth in claim 8, wherein the information comprises the at least one key and corresponding device identification.

11. The device as set forth in claim 8, wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key.

12. The device as set forth in claim 8, wherein the device is selected from the group consisting of a device to connect to a cable network, a direct broadcast satellite (DBS) device, a phone device, an internet device, a broadcast device and a set top box.

13. The device as set forth in claim 8, wherein the device comprises a service provider that communicates data with a second device, the device identification corresponding to the second device.

14. The device as set forth in claim 13, wherein the device is a cable provider headend, a DBS uplink, a digital subscriber line (DSL) center, website and the second device is a set top box.

15. The device as set forth in claim 8, wherein the non-volatile storage medium is selected from the group consisting of FLASH memory, static random access memory (SRAM), hard disk media, memory stick, battery-backed RAM, fuses, nonvolatile removeable media and optical media.

16. The device as set forth in claim 11, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key.

17. The device as set forth in claim 16, wherein the second logic comprises:

a first sub-logic having as input the device identification and a first generation key of the generation keys, said first sub-logic generating a first output;

a second sub-logic having as input the first output and a second generation key of the generation keys, said second sub-logic generating a second output; and

a third sub-logic having as input the second output and a third generation key of the plurality of generation keys, said third sub-logic generation the key as output.

18. The device as set forth in claim 17, wherein the first sub-logic, second sub-logic and third sub-logic are functions selected from the group consisting of logic functions, combinatorial functions and cipher functions.

19. The device as set forth in claim 8, wherein the message is selected from the group consisting of hashing and signing a message and encryption.

20. A system comprising:

at least one first device, said first device comprising;

a non-volatile storage medium for storing information for at least one key corresponding to a device identification of first device,

a first logic to encode data using the at least one key and decode encoded data using the at least one key, and

an input/output to communicate encoded data in a message, the message including the device identification of the first device and the encoded data;

a communication medium; and

at least one second device coupled to the first device through the communication medium, the second device comprising;

a non-volatile storage medium for storing information for at least one key corresponding to a device identification of the first device,

a second logic to encode data using the at least one key and decode encoded data using the at least one key, and

an input/output to communicate encoded data in a message, the message including the device identification of the first device and the encoded data.

21. The system as set forth in claim 20, wherein the second device communicates with a plurality of first devices, the non-volatile storage medium of the second device storing information for at least one key for each first device.

22. The system as set forth in claim 20, wherein the information comprises the at least one key and corresponding device identification.

23. The device as set forth in claim 20, wherein the information comprises generation keys, the generation keys used with the device identification to generate the at least one key.

24. The device as set forth in claim 23, further comprising a second logic, the second logic using the generation keys and the device identification to generate the at least one key.